

### Remarks

Applicant has reviewed the Office Action dated as mailed June 6, 2007 and the documents cited therewith. After the above amendments to the claims have been made, the present application contains claims 1-5, and 7-44. Claims 1, 9, 20, 21, 28, 30, and 38 have been amended. Claims 6 has been canceled.

### Claim Objections

Claims 20 and 28 have been amended to correct the informalities noted in the Office Action. Reconsideration and removal of the objection to claims 20 and 28 is respectfully requested.

### Claim Rejections under 35 U.S.C. §112

Claims 1, 9, 21, 30, and 38 were rejected under 35 U.S.C. § 112, first paragraph, as failing to comply with the enablement requirement. Claims 2-5, 7-8, 10-20, 22-29, 31-37, and 39-44 were rejected for incorporating the deficiencies of independent claims 1, 9, 21, 30, and 38. Claims 1, 9, 21, 30, and 38 were also rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1, 9, 21, 30, and 38 have been amended to comply with the enablement requirement and to more particularly point out and distinctly claim the subject matter of the present invention. Reconsideration and withdrawal of the 35 U.S.C. § 112 rejections of these claims and claims 2-5, 7-8, 10-20, 22-29, 31-37, and 39-44 is respectfully solicited.

### Claim Rejections under 35 U.S.C. §101

Claims 21-29 were rejected under 35 U.S.C. § 101 as being directed to non-statutory subject matter. Specifically, the Office Action indicated that the language of the claim raises a question as to whether the claim is directed merely to an environment or machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under section 101. The Office Action went on to state that the use of a computer is not evident in these claims. Claims 38-44 were further rejected under 35 U.S.C. § 101 because, as

indicated in the Office Action, the claimed invention was directed to the non-statutory subject area of electro-magnetic signals and carrier waves. These rejections are respectfully traversed.

Independent claim 21 has been amended to recite: "a file system protection program operable on a computer..." Thus, the file system protection program is being claimed as part of a computer. As provided by M.P.E.P. § 2106.01, when a computer program is recited in conjunction with a physical structure, such as a computer memory (or the computer itself as recited in amended claim 21), the USPTO personnel should treat the claims as a product claim. Accordingly, Applicant respectfully submits that independent claim 21 recites statutory subject matter under 35 U.S.C. § 101, and reconsideration and withdrawal of the Section 101 rejection of claim 21 is respectfully requested.

Regarding claims 22-29, these claims depend either directly or indirectly from independent claim 21. Therefore, these claims are also submitted to recite statutory subject matter under 35 U.S.C. § 101, and reconsideration and withdrawal of the Section 101 rejection of claims 22-29 is respectfully solicited.

Independent Claim 38 has been amended to recite: "A computer-readable tangible medium having computer-executable instructions for performing a method on a computer..." as clearly illustrated in Figure 2 and as described in paragraph [0028] of the present application, the computer-readable medium 252 is shown as a physical, tangible element that maybe accessed by I/O device 248 which may include disk drives, optical, mechanical, magnetic or infrared input/output devices. Accordingly, computer-readable medium, both on its face and as may be interpreted from the specification, may also refer to a tangible physical medium not to an ethereal "signal". The mere fact that computer program code can be moved from one computer readable storage medium to another does not necessarily indicate that the claims as written and described in the present application are tempting to claim a "signal" per se. The claims have been amended to clearly indicate that the subject matter is tangible with respect to the term "medium" as illustrated in Figure 2 and as may be interpreted from paragraph [0028], thereby excluding the concept of an ethereal "signal" as the medium. Reconsideration and withdrawal of the 35 U.S.C. § 101 rejection of claims 38-44 is respectfully requested.

*Claim Rejections under 35 U.S.C. §102*

Claims 1-2, 5, 7-9, 12-19, 21-30, 32-38, and 40-44 were rejected under 35 U.S.C. § 102(b) as being anticipated by Halperin et al. (U.S. Patent Pub. No. 2002/0194490). This rejection is respectfully traversed.

Claim 1 has been amended to recite:

“flagging a program on a computer as being suspect for possibly containing a virus in response to at least one of:

opening a local file on a local file system of the computer to perform a read operation and opening a shared file on a shared or networked file system to perform a write or append operation with the local file;

the program reading or opening itself and the program attempting to write or append any content to the shared file on the shared or networked file system or to write or append any content to the local file on the local file system;

the program attempting to write or append the local file to the shared or networked file system and preserving a file name of the local file in the shared or networked file system; and

the program attempting to write or append a remote file to the local file system;”

The Office Action cited the Abstract, Paragraphs 73-77 and 88-108 of Halperin for rejecting these features of claim 1. As described below, Applicant respectfully submits that Halperin does not teach or suggest the specific conditions for flagging a program on a computer as being suspect for possibly containing a virus as required by the embodiment of the present invention as recited in claim 1.

The abstract of Halperin recites:

“A method for malicious software detection including grouping a plurality of computing devices in a network into at least two groups, measuring a normal operation value of at least one operating parameter of any of the groups and detecting a change in the value to indicate possible malicious software behavior within the network.”

Accordingly, from the abstract of Halperin, Halperin teaches detection of malicious software in a plurality of computing devices within a network and not within an individual computer as provided by the present invention. Halperin does not teach or suggest flagging a program on a computer as being suspect for possibly containing a virus, nor does Halperin teach or suggest the specific conditions associated with the computer for flagging the program on the computer as provided by the embodiment of the present invention as recited in claim 1.

Paragraphs 73-77 of Halperin, also cited in the Office Action in rejecting claim 1, recite:

“[0073] Reference is now made to FIG. 2, which is a simplified flow chart illustration of an exemplary method of operation of the system FIG. 1, useful in understand the present invention. In the method of FIG. 2, computer 100 becomes infected by a computer virus such as by receiving the virus by another computer via network 102 or via the introduction of infected data storage media such as a diskette or a compact disc into computer 100. As the virus attempts propagate it selects one or more valid and decoy addresses from address book 102 in folders 104, automatically generates messages that incorporate the virus, typically as an attachment, and forwards the messages to server 108. Server 108 scans messages received from computer 100. Should server 108 detect a message addressed to a decoy address, server 108 may initiate one or more virus containment actions such as, but not limited to:

[0074] Suspending any or all messages sent by computer 100, thereby preventing messages sent by computer 100 from being forwarded to recipients.

[0075] Forwarding messages that are addressed to a decoy address to a third party for analysis, such as a company or other body that produces anti-virus software.

[0076] Notifying a user at computer 100 of the suspicious message activity.

[0077] Notifying a system administrator that a virus may have been detected.”

(emphasis added)

Thus, Halperin teaches sending messages across a network from a computer 100 to a server 108, scanning the messages received from computer 100 on the server 108, and if the server 108 detects a message addressed to a decoy address, server 108 may initiate one or more virus containment actions such as those recited above. Halperin teaches suspending messages being sent by an infected computer but Halperin does not teach or suggest flagging a program on the computer based on specific local file system operations as provided by the embodiment of the present invention as recited in claim 1. Applicant further respectfully submits that there is no teaching or suggestion in Halperin of the specific local file system operations being performed on the computer for determining whether to flag a program on the computer as being suspect for possibly containing a virus. Halperin merely teaches initiating virus scanning and virus containment actions at the server and network level as opposed to the computer level as required by the embodiment of the present invention as recited in claim 1.

In rejecting claim 1, the Office Action on page 10 also cited the following from paragraphs 97-107 of Halperin:

“After collecting information regarding target behavior detected at two or more computers 500, server 502 may then correlate the presence of target behavior detected at two or more computers 500 in order to determine whether the correlated target behavior corresponds to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers. Any known behavior correlation technique may be used such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers... [0107] Upon detecting a suspicious behavior pattern server 502 may initiate one or more virus containment actions such as described hereinabove with reference to FIG.2.”  
(emphasis added)

Accordingly, Halperin teaches collecting information regarding target behavior detected at two or more computers 500 by the server 502. Then the server 502 correlates the presence of the target behavior to determine whether the correlated target behavior corresponds to a predefined suspicious behavior as an indication that a computer virus may have infected those computers. Applicant respectfully submits that there is no teaching or suggestion in Halperin of flagging a program on an individual computer as being suspect for possibly containing a virus. Additionally, Halperin does not teach or suggest the specific conditions or file system operations as recited by the embodiment of the present invention in claim 1 for flagging the program on the computer. Namely, Halperin does not teach or suggest opening a local file on a local file system of the computer to perform a read operation and opening a shared file on a shared or network file system to perform a write or append operation with the local file as a condition for flagging a program on a computer as being suspect for possibly containing a virus. Nor does Halperin teach or suggest the program reading or opening itself and the program attempting to write or append any content to the shared file on the shared or network file system or to write or append any content to the local file on the local file system for flagging a program on the computer. Nor does Halperin teach or suggest the program attempting to write or append the local file to the shared or network file system and preserving a file name of the local file in the shared or network file system for flagging a program, as required by the embodiment of the present invention as recited in claim 1.

Additionally, claim 1 recites: “storing a file name and a location where the local or shared file is copied or written in response to the local or shared file being copied or written by the

program.” The Office Action cited paragraph [0108] of Halperin for rejecting this feature of claim

1. Paragraph [0108] of Halperin recites:

“[0108] In the system and methods described hereinabove with reference to FIGS. 1, 2, 3, 4, 5, and 6, the server may include a buffer or other mechanism whereby messages received from the computer are held, typically for a predefined delay period prior to forwarding the messages to their intended recipients. In this way, should a computer virus send one or more infected messages to valid, non-decoy addresses before sending an infected messages to a decoy address, the infected messages to valid, non-decoy addresses that are still held at the server may be ‘quarantined’ at the server and thus prevented, together with the infected message to a decoy address, from reaching their intended destinations.”

Accordingly, Applicant respectfully submits that Halperin teaches away from the present invention in that Halperin quarantines the messages and does not allow them to reach their intended destinations. In contrast, the present invention, as recited in the embodiment of claim 1, permits the file to be copied or written by the program at its intended location and then stores the file name and location where the local or shared file is copied or written. In contrast, Halperin teaches storing an entire message, not merely a name or identification of the message, in a buffer associated with the server. The message is not allowed to be sent to its intended destination. Accordingly there is no need for Halperin to store a file name and a location where the file is copied or written and Halperin does not teach or suggest such as provided by the embodiment of the present invention as recited in claim 1.

For all of the reasons discussed above, the Applicant respectfully submits that claim 1 is patentably distinguishable over Halperin, and reconsideration and withdrawal of the 35 U.S.C. §102 rejection of claim 1 is respectfully requested.

Turning now to the rejection of claims 2, 5, 7, and 8, these claims depend either directly or indirectly from independent claim 1. Because of this dependency, these claims contain all of the features of independent claim 1. Therefore, these claims are also submitted to be patentably distinguishable over Halperin, and reconsideration and withdrawal of the Section 102 rejection of these claims is respectfully solicited.

Regarding the rejection of independent claim 9 under 35 U.S.C. § 102(b) as being anticipated by Halperin, claim 9 has been amended to recite: “logging any predetermined file system operations associated with the program including recording a file name and a location where a file is written in response to the file being written.” The Office Action cited paragraph [0108] in rejecting

this feature of claim 9. As previously discussed, Halperin teaches in paragraph [0108] quarantining at a server messages believed to contain a virus. In contrast, the present invention as recited in claim 9 permits the file to be written and then records the file name and the location where the file is written. As discussed above, Halperin does not teach or suggest this feature of the present invention. Accordingly, claim 9 is submitted to be patentably distinguishable over Halperin, and reconsideration and withdrawal of the 35 U.S.C. § 102 rejection of claim 9 is respectfully requested.

Turning now to the rejection of claims 12-19 under 35 U.S.C. § 102(b) as being anticipated by Halperin, these claims recite additional features which further patentably distinguish over Halperin. For example, claim 15 recites flagging a program in response to different file system operations similar to those recited in independent claim 1. As discussed with respect to independent claim 1, Halperin does not teach or suggest the specific features recited in dependent claim 15.

Additionally, claims 12-19 depend either directly or indirectly from independent claim 9, and by virtue of the dependency, contain all of the features of independent claim 9. Therefore, claims 12-19 are also submitted to be patentably distinguishable over Halperin, and reconsideration and withdrawal of the Section 102 rejection of claims 12-19 is respectfully solicited.

With regard to the rejection of independent claim 21 under 35 U.S.C. § 102(b) as being anticipated by Halperin, claim 21 recites similar features to independent claim 9. Therefore, claim 21 is submitted to be patentably distinguishable over Halperin for the same reasons as discussed with respect to independent claim 9. Reconsideration and withdrawal of the Section 102 rejection of claim 21 is respectfully requested.

Regarding the rejection of claims 22-29 under 35 U.S.C. § 102(b) as being anticipated by Halperin, these claims recite additional features which further patentably distinguish over Halperin. For example, claim 23 recites: "a log to record any predetermined file system operations." In contrast, Halperin merely teaches quarantining any messages being sent across a network by a server and does not teach or suggest a log to record predetermined file system operations. Additionally, claim 24 recites means to flag the other program in response to specific operations similar to those recited in independent claim 1 and which are not taught or suggested by Halperin.

Additionally, claims 22-29 depend either directly or indirectly from independent claim 21. Because of this dependency, claims 22-29 include all of the features of independent claim 21. Therefore, these claims are also submitted to be patentably distinguishable over Halperin, and

reconsideration and withdrawal of the 35 U.S.C. § 102 rejection of claims 22-29 is respectfully solicited.

Turning now to the rejection of independent claim 30 under 35 U.S.C. § 102 (b) as being anticipated by Halperin, claim 30 recite similar features to independent claims 9 and 21. Therefore, independent claim 30 is submitted to be patentably distinguishable over Halperin for the same reasons as discussed with respect to independent claims 9 and 21.

Regarding the rejection of claims 32-37, these claims recite additional features which further patentably distinguish over Halperin. For example, claim 33 recites means to flag the other program in response to at least one of specific operations similar to those recited in independent claim 1 which are neither taught nor suggested by Halperin as discussed with respect to independent claim 1. Additionally, claims 32-37 depend either directly or indirectly from independent claim 30, and by virtue of this dependency, claim all of the features of independent claim 30. Therefore, claims 32-37 are submitted to be patentably distinguishable over Halperin, and reconsideration and withdrawal of the Section 102 rejection of claims 32-37 is respectfully solicited.

Turning now to the rejection of independent claim 38 under 35 U.S.C. § 102(b) as being anticipated by Halperin, independent claim 38 includes features similar to independent claim 9. Therefore, claim 38 is submitted to be patentable distinguishable over Halperin for the same reasons as discussed with respect to independent claim 9.

With respect to the rejection of claims 40-44 under 35 U.S.C. § 102(b) as being anticipated by Halperin, these claims recite additional features which further patentably distinguish over Halperin. Additionally, these claims depend either directly or indirectly from independent claim 38. By virtue of this dependency, claims 40-44 include all of the features of independent claim 38. Therefore, these claims are also submitted to be patentably distinguishable over Halperin, and reconsideration and withdrawal of the Section 102 rejection of these claims is respectfully requested.

#### **Claim Rejections under 35 U.S.C. §103**

Claims 3-4, 10-11, 20, 22, 31, and 39 were rejected under 35 U.S.C. §103(a) as being unpatentable over Halperin et al. as applied to claims 1-2, 5, 7-9, 21-30, 32-38, and 40-44, and in view of Satterlee et al. (US Patent Pub. No. 2004/0025015). This rejection is respectfully traversed.



Applicant respectfully submits that this rejection under 35 U.S.C. §103 does not follow the M.P.E.P. §706.02(j) which states:

“After indicating that the rejection is under 35 U.S.C. §103, the examiner should set forth in the Office Action: . . . (B) the difference or differences in the claim over the applied reference(s), (C) the proposed modification of the applied reference(s) necessary to arrive at the claimed subject matter, and (D) an explanation of why one of ordinary skill in the art at the time the invention was made would have been motivated to make the proposed modification . . . The teaching or suggestion to make the claimed combination and the reasonable expectation of the success must both be found in the prior art and not based on applicant’s disclosure.” *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

As discussed in detail below, Applicant respectfully submits that there is no teaching or suggestion in Halperin and Satterlee that their teachings may be combined so as to provide the present invention as recited in the claims.

Satterlee teaches a method and system for the managed security control of processes on a computer system. A protector system implements a two-step process to ensure that software programs do not perform malicious activities which may damage the computing device or other computing resources to which the device is coupled. In the first phase, the protector system determines whether a software program has been previously approved and validates that the software program has not been altered. If the software program is validated during the first phase, this will minimize or eliminate security monitoring operations while the software program is executing during the second phase. See the abstract of Satterlee.

Accordingly, Satterlee involves protecting a computing device from malicious activities within the computing device. In contrast, Halperin discloses a system and method of virus containment in computer networks. In paragraph [0073] of Halperin, Halperin recites:

“In the method of FIG.2, computer 100 becomes infected by a computer virus, such as by receiving the virus from another computer via a network 102 or via the introduction of infected data storage media such as a diskette or compact disc into computer 100. As the virus attempts to propagate it selects one or more valid and decoy addresses from address book 102 and folders 104, automatically generates messages that incorporate the virus, typically as an attachment, and forwards the messages to server 108. Server 108 scans messages received from computer 100. Should server 108 detect a message addressed to a decoy address, server 108 may initiate one or more virus containment actions...”

Accordingly, Halperin is concerned with detecting message that may contain viruses being transmitted across a network. The messages are scanned at a server 108 not at the computer 100 and if a message is detected to a decoy address, server 108 initiates the virus containment action. Thus, Halperin operates at the server or network level and not at the computing device level as taught by Satterlee. Accordingly, Applicant respectfully submits that a person of ordinary skill in the art would not be motivated to combine the teachings of Satterlee with Halperin.

Even if it were proper to combine the teachings of Satterlee and Halperin, they still would not provide the present invention as recited in the claims. Claims 3-4 depend directly from independent claim 1; claims 10-11 and 20 depend either directly or indirectly from independent claim 9; claim 22 depends directly from independent claim 21; claim 31 depends directly from independent claim 30; and claim 39 depends directly from independent claim 38. By virtue of these dependencies, these claims contain all of the features of the respective, referenced independent claim. Applicant respectfully submits that Satterlee adds nothing to the teachings of Halperin so as to render independent claims 1, 9, 21, 30, and 38 unpatentable. Accordingly, claims 3-4, 10-11, 20, 22, 31, and 39 are submitted to be patentable distinguishable over Halperin and Satterlee, and reconsideration and withdrawal of Section 103 rejection of these claims is respectfully requested.

Conclusion

For the foregoing reasons, the Applicant respectfully submits that all of the claims in the present application are in condition for allowance. Reconsideration and withdrawal of the rejections and allowance of the claims at the earliest possible date are respectfully solicited.

If the Examiner has any questions about the present Amendment or anticipates finally rejecting any claim of the present application, a telephone interview is requested.

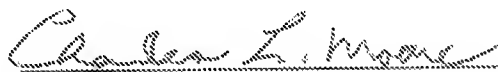
If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 09-0461.

Respectfully submitted,

James E. Aston, et al.  
(Applicant)

Date: Sept. 4, 2007

By:



Charles L. Moore  
Registration No. 33,742  
Moore & Van Allen, PLLC  
P.O. Box 13706  
Research Triangle Park, N.C. 27709  
Telephone: (919) 286-8000  
Facsimile: (919) 286-8199